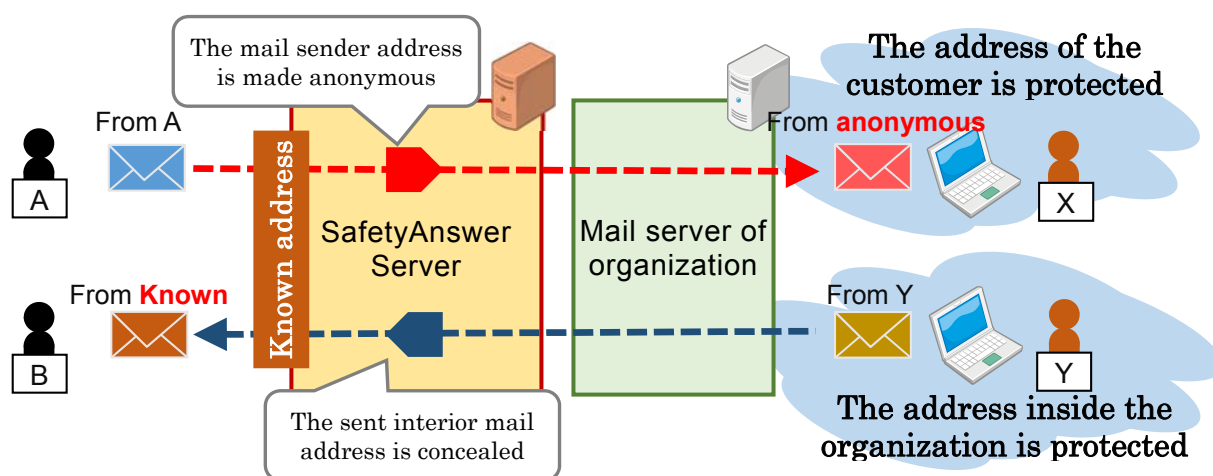


SafetyAnswer

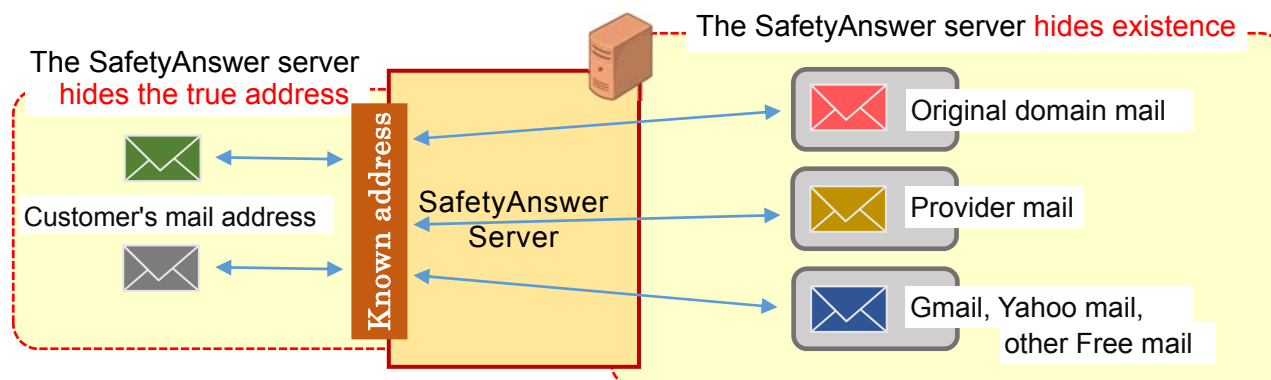
1. The mail server against which a mail address is defended

SafetyAnswer can stop a leak of a target mail address of various security attack by that a mail address of a mail sender is made anonymous using the original technology which concealment-izes a mail address and that the user's mail address which receives a mail actually is concealed.



Without using an exclusive mail server, it's possible to use and use the mail address the provider offers and a mail address of free mail service as the address of the interior.

A mail for the domain is sent by that a **SafetyAnswer** server processes an acquired mail for the domain to the mail service each user uses. **SafetyAnswer** judges a right mail address, and for a mail to be sent to the mail each user sends from the opening to the public address, a mail address of the mail service each user uses doesn't leak.

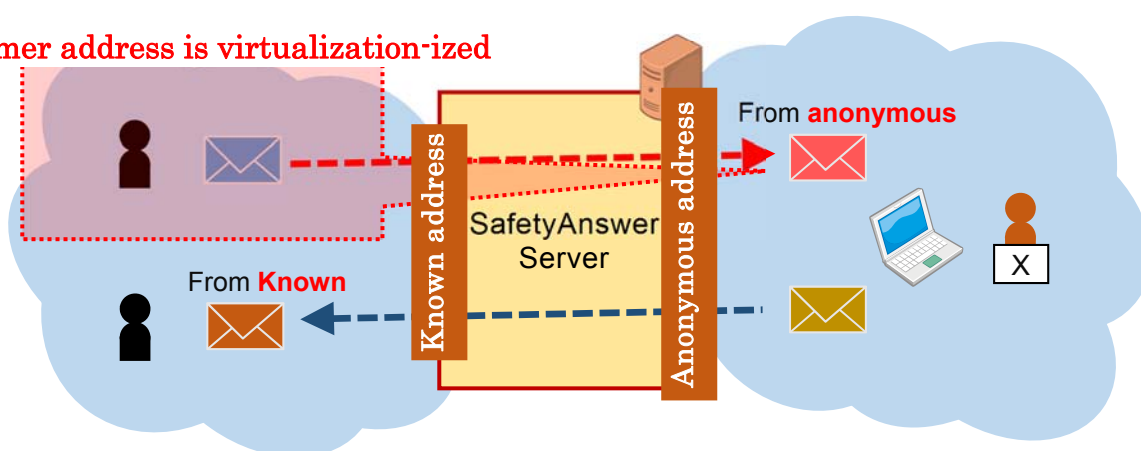


2. The mail address is virtualization-ized

The **SafetyAnswer** server produces the virtual environment of the mail service which makes customer's mail address and a mail address inside the organization circulated at the price different from the actual mail address using technology that the sender address of the reception and the sent mailing is concealed.

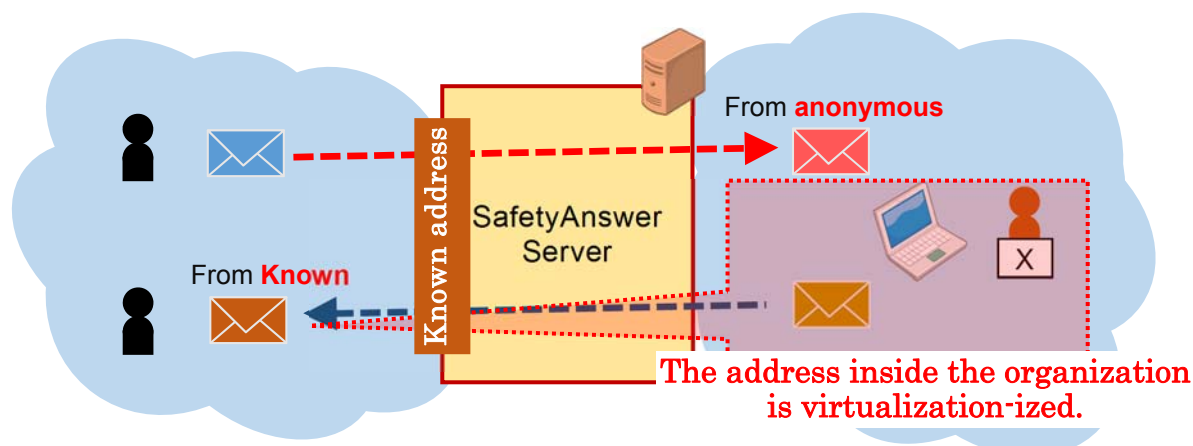
The Phantom function

Customer address is virtualization-ized



The customer's mail address which collects inside the organization is virtualization-ized by the customer's mail address's which is being sent being made anonymous.

The stealth function



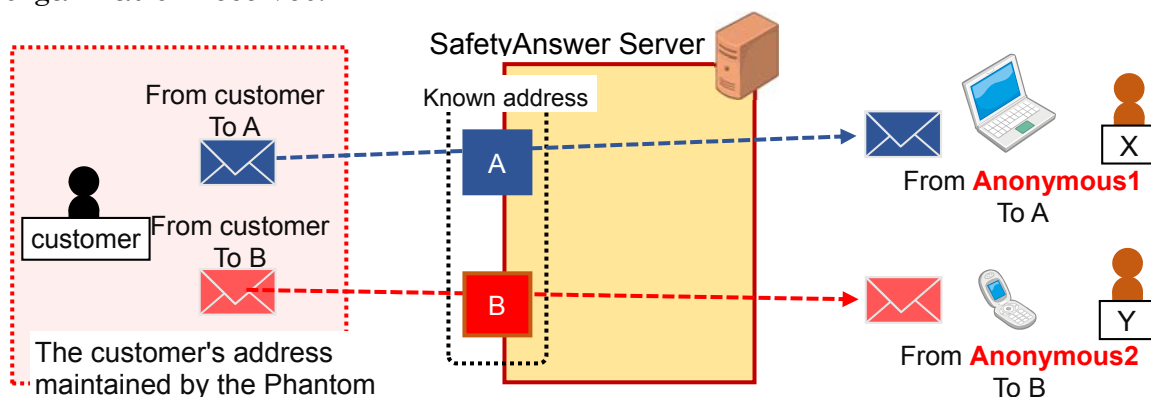
The true address of the user a transmission (answer) mails is virtualization-ized by the address's receiving a mail actually inside the organization being concealed.

(1) The Phantom Function

The mail address which reaches from outside isn't collected.

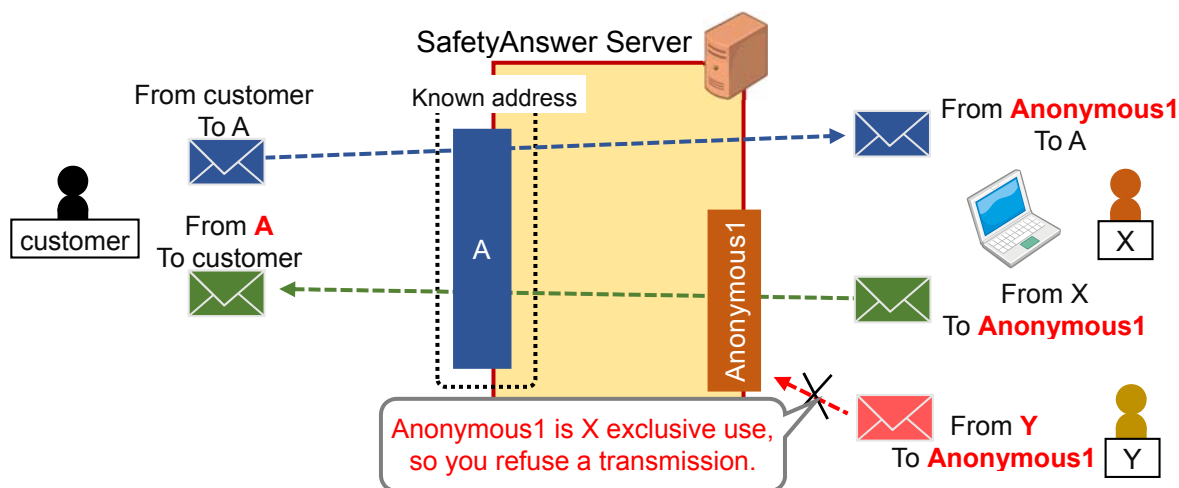
Everybody can't know, so customer's true mail address doesn't leak.

A mail from the customer the **SafetyAnswer** server received by the managed opening to the public address can make the mail sender address anonymous and forward. The mail sender address is made anonymous, and the user of **SafetyAnswer** received inside the organization receives.



When the known address even a mail from the same customer receives is different, it's made by the different address anonymous.

The user of **SafetyAnswer** who has received a mail is that anonymity sends a mail from its mail address to the address, and a **SafetyAnswer** server returns an address to customer's true mail address and delivers a mail correctly.



It isn't possible to send a mail to a customer from the different address which isn't the address which received the customer's mail which became anonymous at this time. Even the inside of the company will be others, and it's finished and mailing is sent unjustly, but it's said that this isn't made.

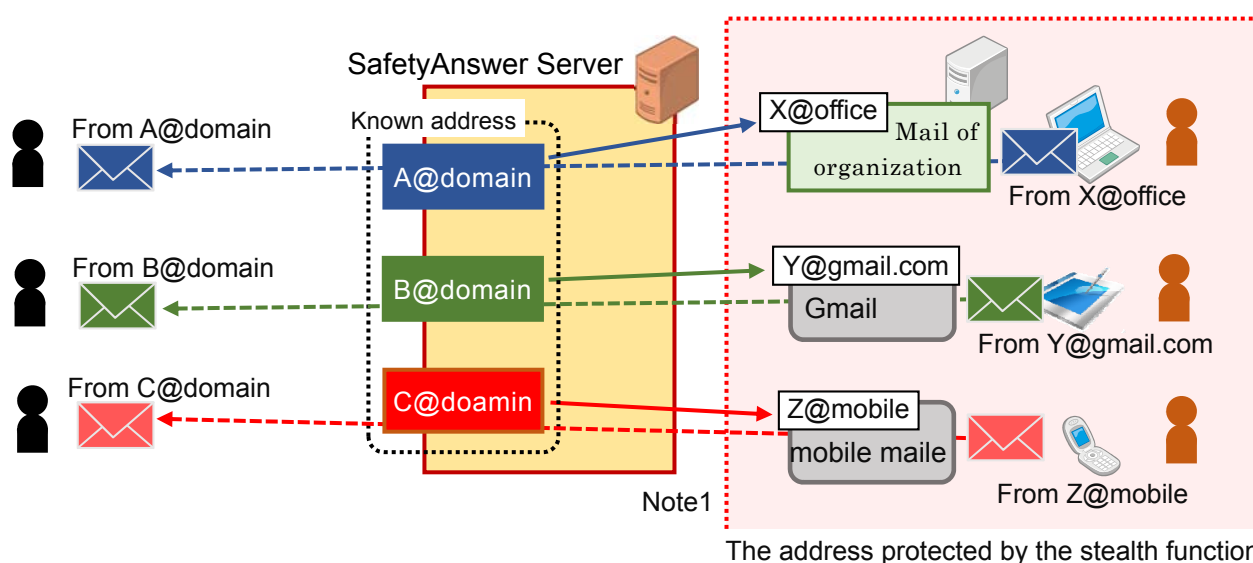
The mail sender received by the Phantom function will be the existence just like a ghost only himself who has received a mail sees.

(2) The Stealth Function

The mail address used at the inside of the organization can't use in outside.
A target of targeted attack mail doesn't leak out to outside.

SafetyAnswer server forwards the mail delivered to the known address to the mail address that was set in the transfer destination. The address of the real mail recipient who is ahead of the known address isn't known of to the sender sending a mail from outside.

And the known address will be the mailer address by the user's using the mail address from which he hides behind the known address sending a mail via a SafetyAnswer server, and a mail is sent, and the address of the true mail sender isn't known the recipient who has received a mail.



It's possible to be to use **SafetyAnswer** and conceal the mail address to which reception is sending a mail inside the organization.

Even free mail of a carrier mail of the mail address the provider offers, the mail address used by the original domain and the carrying, Gmail and a Yahoo mail can use the mail address used inside the organization.

Note 1) when change can't make the server when a mail sends, a **SafetyAnswer** server, it's necessary to send a mail by "reply operation" to incoming mail. A cell phone mail is generally relevant to this. The answer operation on the mail received through a **SafetyAnswer** server by all cases is real, a mail, it'll be the answer mail which made the opening to the known address the sender address, not the address I answered.

The user's existence to which reception is sending a mail inside the organization will be the existence which was hidden from the mail user who is outside the organization by the stealth function.